

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

#3
Jc929 U.S. PTO
09/800505
03/08/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application:

1998年 9月18日

出願番号
Application Number:

平成10年特許願第265210号

出願人
Applicant(s):

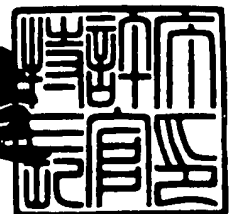
富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年12月 1日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2000-3098709

3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:)
Seigo KOTANI, et al.)
Application No.: To be Assigned) Group Art Unit: To be Assigned
Filed: March 8, 2001) Examiner: To be Assigned
For: INFORMATION MANAGEMENT METHOD AND INFORMATION MANAGEMENT

1c929 U.S. PTO
09/800505
03/08/01

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN
APPLICATION IN ACCORDANCE
WITH THE REQUIREMENTS OF 37 C.F.R. §1.55

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. §1.55, the applicant(s) submit(s)
herewith a certified copy of the following foreign application:

Japanese Patent Application No. 10-265210
Filed: September 8, 1998

It is respectfully requested that the applicant(s) be given the benefit of the foreign
filing date as evidenced by the certified papers attached hereto, in accordance with the
requirements of 35 U.S.C. §119.

Respectfully submitted,
STAAS & HALSEY LLP

By: _____
James D. Halsey, Jr.
Registration No. 22,729

700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500
Date: 3/7/01

【書類名】 特許願

【整理番号】 9890536

【提出日】 平成10年 9月18日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 12/14

【発明の名称】 情報管理方法および情報管理装置

【請求項の数】 26

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 小谷 誠剛

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 長谷部 高行

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 平野 秀幸

【特許出願人】

 【識別番号】 000005223

 【氏名又は名称】 富士通株式会社

【代理人】

 【識別番号】 100094145

 【弁理士】

 【氏名又は名称】 小野 由己男

 【連絡先】 0 6 - 3 5 5 - 5 3 5 5

【選任した代理人】

 【識別番号】 100094167

【弁理士】

【氏名又は名称】 宮川 良夫

【選任した代理人】

【識別番号】 100106367

【弁理士】

【氏名又は名称】 稲積 朋子

【手数料の表示】

【予納台帳番号】 020905

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9807456

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報管理方法および情報管理装置

【特許請求の範囲】

【請求項 1】

媒体固有の情報を有する記録媒体上の所定の領域に格納された所定の情報を、前記媒体固有の情報またはそれに基づいて生成された鍵により暗号化して前記所定の領域外に導出する情報管理方法。

【請求項 2】

前記記録媒体は、前記所定の情報を格納する第 1 領域と、前記第 1 領域と異なる第 2 領域とを備える、請求項 1 に記載の情報管理方法。

【請求項 3】

前記第 2 領域は外部からの指令に基づいて任意の情報を書込・読出可能なユーザ利用領域であり、前記第 1 領域は外部からの指令に基づいて制御することが不可能な機密領域である、請求項 2 に記載の情報管理方法。

【請求項 4】

前記第 2 領域に格納される任意の情報は暗号化された電子化データであり、前記第 1 領域に格納される所定の情報は前記電子化データを利用する利用権に基づく許諾情報を含む、請求項 3 に記載の情報管理方法。

【請求項 5】

前記所定の情報は、前記媒体固有の情報またはそれに基づいて生成された鍵により暗号化されて前記所定の領域に格納されている、請求項 2～4 のいずれかに記載の情報管理方法。

【請求項 6】

前記所定の情報は、前記記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵により暗号化されている、請求項 5 に記載の情報管理方法。

【請求項 7】

前記暗号化された所定の情報を前記第 2 領域に格納する、請求項 2～6 のいずれかに記載の情報管理方法。

【請求項 8】

前記第2領域に格納されている暗号化された所定の情報を前記媒体固有の情報またはそれに基づいて生成された鍵により復号化し、前記第1領域に格納されている所定の情報を更新する、請求項7に記載の情報管理方法。

【請求項9】

前記所定の情報を前記第1領域外に導出する際に、前記媒体固有の情報またはそれに基づいて生成された鍵および前記記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵により暗号化する、請求項7に記載の情報管理方法。

【請求項10】

前記第2領域に格納されている暗号化された所定の情報を、前記記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵および前記媒体固有の情報またはそれに基づいて生成された鍵により復号化して、前記第1領域に格納されている所定の情報を更新する、請求項9に記載の情報管理方法。

【請求項11】

前記暗号化された所定の情報を、前記記録媒体とは異なる第2の記録媒体上に格納する、請求項1～6のいずれかに記載の情報管理方法。

【請求項12】

前記第2の記録媒体に格納されている暗号化された所定の情報を前記媒体固有の情報またはそれに基づいて生成された鍵により復号化し、前記所定の領域に格納されている所定の情報を更新する、請求項11に記載の情報管理方法。

【請求項13】

前記所定の情報を前記第2の記録媒体上に導出する際に、前記媒体固有の情報またはそれに基づいて生成された鍵および前記第2の記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵により暗号化する、請求項11に記載の情報管理方法。

【請求項14】

前記第2の記録媒体に格納されている暗号化された所定の情報を、前記第2の記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵および前記媒体固有の情報またはそれに基づいて生成された鍵により復号化して、前記

所定の領域に格納されている所定の情報を更新する、請求項 13 に記載の情報管理方法。

【請求項 15】

前記媒体固有の情報は前記記録媒体から電子的に入手できるとともに可視的に前記記録媒体上に表示されている、請求項 1 ～ 14 にいずれかに記載の情報管理方法。

【請求項 16】

前記記録媒体を駆動する装置に固有の情報は、前記装置から電子的に入手できるとともに可視的に前記装置上に表示されている、請求項 6、9 または 10 に記載の情報管理方法。

【請求項 17】

前記第 2 の記録媒体を駆動する装置に固有の情報は、前記装置から電子的に入手できるとともに可視的に前記装置上に表示されている、請求項 13 または 14 に記載の情報管理方法。

【請求項 18】

媒体固有の情報を有し、外部からの指令に基づいて任意の情報を書込・読出可能なユーザ利用領域と、外部からの指令に基づいて制御することが不可能な機密領域とを備え、前記ユーザ利用領域に格納された任意の情報に対する利用権に基づく許諾情報が前記機密領域に格納されている記録媒体の情報を管理する情報管理装置であって、

前記ユーザ利用領域に対して任意の情報を書込・読出を行う書込・読出手段と

前記機密領域に格納されている許諾情報を前記媒体固有の情報またはそれに基づいて生成された鍵により暗号化して前記機密領域外に導出する所定情報導出手段と、

を備える情報管理装置。

【請求項 19】

前記暗号化された許諾情報を、前記書込・読出手段により前記ユーザ利用領域に格納する、請求項 18 に記載の情報管理装置。

【請求項 20】

前記ユーザ利用領域に格納されている暗号化された許諾情報を前記媒体固有の情報により復号化して前記機密領域に格納されている許諾情報を更新する所定情報更新手段をさらに備える、請求項 19 に記載の情報管理装置。

【請求項 21】

装置固有の情報を備え、前記所定情報導出手段は、前記許諾情報を前記媒体固有の情報またはそれに基づいて生成された鍵および前記装置に固有の情報またはそれに基づいて生成された鍵により暗号化する、請求項 18 または 19 に記載の情報管理装置。

【請求項 22】

前記ユーザ利用領域に格納されている暗号化された許諾情報を前記装置に固有の情報またはそれに基づいて生成された鍵および前記媒体固有の情報またはそれに基づいて生成された鍵により復号化して前記機密領域に格納されている許諾情報を更新する所定情報更新手段をさらに備える、請求項 21 に記載の情報管理装置。

【請求項 23】

前記所定情報導出手段は、前記暗号化された許諾情報を前記記録媒体とは異なる第 2 の記録媒体に送出する、請求項 18 に記載の情報管理装置。

【請求項 24】

前記第 2 の記録媒体に格納されている暗号化された許諾情報を前記媒体固有の情報により復号化して前記機密領域に格納されている許諾情報を更新する所定情報更新手段をさらに備える、請求項 23 に記載の情報管理装置。

【請求項 25】

前記第 2 の記録媒体を駆動する装置は装置固有の情報を備え、前記所定情報導出手段は、前記許諾情報を前記媒体固有の情報またはそれに基づいて生成された鍵および前記第 2 の記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵により暗号化する、請求項 23 に記載の情報管理装置。

【請求項 26】

前記第 2 の記録媒体に格納されている暗号化された許諾情報を、前記第 2 の記

録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵および前記媒体固有の情報またはそれに基づいて生成された鍵により復号化して前記機密領域に格納されている許諾情報を更新する所定情報更新手段をさらに備える、請求項 25 に記載の情報管理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報管理方法および情報管理装置に関し、特に、媒体固有の情報を有する記録媒体に対して任意の情報を記録・読出を行う際の情報管理方法およびその装置に関する。

【0002】

【従来の技術】

コンピュータプログラムなどのソフトウェアや電子出版物では、光磁気ディスク（MO）、デジタルビデオディスク（DVD）、フロッピーディスク（FD）、ミニディスク（MD）、その他の記録媒体上に電子化データを格納して販売される。このような電子化データは、一般にコピーが容易であり、不正コピーが頻繁に行われている。このため、ソフトウェアベンダーや出版者側の著作権が侵害され著しく利益が阻害されるおそれがある。

【0003】

このような記録媒体上に格納された電子化データを保護するために、ユーザ固有の情報を用いて暗号化した許諾情報を生成し、これを記録媒体上の所定の領域に格納して配布することが提案されている。ソフトウェアや出版物などの電子化データは、所定の暗号鍵によって暗号化されて記録媒体上に格納されている。また、この暗号化された電子化データを復号化するための復号鍵がユーザ固有の情報を用いて暗号化され、許諾情報として記録媒体上に格納されている。

【0004】

ユーザ側では、この許諾情報をユーザ固有の情報により復号化することによって復号鍵を得ることができ、記録媒体上に格納されている暗号化された電子化データをこの復号鍵を用いて復号化して利用することができる。

このように構成することによって、ユーザ個々に電子化データの利用権を与える際に、電子化データを暗号化するための暗号鍵を共通にすることができ、ユーザ毎に異なるユーザ固有の情報を用いて復号鍵を暗号化することによって、利用権を個々に与えることが可能となる。

【0005】

ここで用いられるユーザ固有の情報とは、例えば、ユーザが使用しているコンピュータまたは記録媒体を駆動する装置に付与されている装置番号である。したがって、ユーザが正規に入手したものであっても、異なる装置では使用できなくなり、この記録媒体を譲渡することもできないという不都合がある。

特開平5-257816号公報には、記録媒体にこの媒体固有の情報を与え、暗号化された電子化データを復号するための復号鍵をこの媒体固有の情報により暗号化して記録媒体に格納するようにした方法が提案されている。

【0006】

この場合、前述の場合と同様に、電子化データを暗号化する際の暗号鍵を共通にすることができ、ユーザ毎に異なる媒体固有の情報を用いて復号鍵を暗号化することによって、利用権を個々に与えることが可能となる。

【0007】

【発明が解決しようとする課題】

上述のような方法においては、暗号化された電子化データは、ユーザがアクセス可能な領域に格納される。また、この電子化データを利用するための許諾情報は、ユーザがアクセス不可能な機密領域に格納される。したがって、正規のユーザであっても許諾情報を読み出してバックアップをとることができず、この機密領域に格納されているデータがなんらかの障害により破壊された場合には、電子化データを利用することができなくなる。このような場合には、ソフトウェアベンダーや出版者、その代理店などの電子化データの管理者による利用権の再発行が必要となる。したがって、この再発行の手続きに煩雑な作業と余分なコストを必要とすることとなる。

【0008】

本発明は、記録媒体上に格納された電子化データを利用するために必要な許諾

情報がなんらかの障害により破壊された場合であっても、ユーザがバックアップ情報を用いてこれを復帰させることが可能な情報管理方法および情報管理装置を提供することを目的とする。

【0009】

【課題を解決するための手段】

本発明に係る情報管理方法は、媒体固有の情報に有する記録媒体上の所定の領域に格納された所定の情報を、媒体固有の情報またはそれに基づいて生成された鍵により暗号化して所定の領域外に導出する。

ここで、記録媒体は、所定の情報を格納する第1領域と、第1領域と異なる第2領域とを備える構成とすることができる。

【0010】

また、第2領域は外部からの指令に基づいて任意の情報を書込・読出可能なユーザ利用領域であり、第1領域は外部からの指令に基づいて制御することが不可能な機密領域で構成することができる。

この場合、第2領域に格納される任意の情報は暗号化された電子化データであり、第1領域に格納される所定の情報は電子化データを利用する利用権に基づく許諾情報を含むように構成できる。

【0011】

また、所定の情報は、媒体固有の情報またはそれに基づいて生成された鍵により暗号化されて所定の領域に格納される構成とすることができる。

さらに、所定の情報は、記録媒体を駆動する装置に固有の情報に基づいて暗号化される構成であってもよい。

また、暗号化された所定の情報を第2領域に格納する構成とすることができる。

【0012】

この場合、第2領域に格納されている暗号化された所定の情報を媒体固有の情報またはそれに基づいて生成された鍵により復号化し、第1領域に格納されている所定の情報を更新するように構成できる。

また、所定の情報を第1領域外に導出する際に、媒体固有の情報またはそれに

基づいて生成された鍵および記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵により暗号化するように構成できる。

【0013】

この場合には、第2領域に格納されている暗号化された所定の情報を、記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵および媒体固有の情報またはそれに基づいて生成された鍵により復号化して、第1領域に格納されている所定の情報を更新するように構成できる。

上述のような構成とすることによって、所定の情報を格納されている所定の領域外に導出する場合には、この媒体に固有の情報により暗号化されているので、他の記録媒体にコピーしても、これを復号化することが困難である。例えば、第2領域にソフトウェアや出版物などの電子化データを格納する際に、この電子化データを暗号鍵により暗号化して格納しておき、これを復号するための復号鍵をこの記録媒体に固有の情報で暗号化してユーザのアクセス不可能な第1領域に格納しておけば、暗号化するための暗号鍵をユーザ個々に変える必要がなく、共通の暗号鍵を用いて暗号化して格納できる。第1領域に格納されている暗号化された復号鍵は、さらに媒体固有の情報を用いて暗号化されて、第1領域外に導出するように構成しているため、ユーザのバックアップとして保存しておくことが可能である。この保存されたバックアップデータは、媒体固有の情報により暗号化されているため、これを他の記録媒体にコピーしても復号化することが困難であり、電子化データを復号するための復号鍵を得ることは困難である。

【0014】

また、所定の領域に格納されている情報が破壊されてもこのバックアップデータに基づいてユーザ側で許諾情報を復元することが可能であり、煩わしい利用権の再発行の手続きを必要としない。

また、暗号化された所定の情報を、記録媒体とは異なる第2の記録媒体上に格納するように構成できる。

【0015】

この場合、第2の記録媒体に格納されている暗号化された所定の情報を媒体固有の情報またはそれに基づいて生成された鍵により復号化し、所定の領域に格納

されている所定の情報を更新するように構成できる。

また、所定の情報を第2の記録媒体上に導出する際に、媒体固有の情報またはそれに基づいて生成された鍵および第2の記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵により暗号化するように構成できる。

【0016】

この場合には、第2の記録媒体に格納されている暗号化された所定の情報を、第2の記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵および媒体固有の情報またはそれに基づいて生成された鍵により復号化して、所定の領域に格納されている所定の情報を更新するように構成できる。

また、媒体固有の情報は記録媒体から電子的に入手できるとともに可視的に記録媒体上に表示されていることが好ましく、記録媒体を駆動する装置に固有の情報および第2の記録媒体を駆動する装置に固有の情報は、装置から電子的に入手できるとともに可視的に装置上に表示されていることが好ましい。

【0017】

この場合には、前述したような許諾情報のバックアップデータを第2の記録媒体に保存しておき、第1領域に格納されたデータが破壊されたときに、この第2の記録媒体に格納された情報に基づいて、これを復元することが可能となる。

本発明に係る情報管理装置は、媒体固有の情報を有し、外部からの指令に基づいて任意の情報を書込・読出可能なユーザ利用領域と、外部からの指令に基づいて制御することが不可能な機密領域とを備え、ユーザ利用領域に格納された任意の情報に対する利用権に基づく許諾情報が機密領域に格納されている記録媒体の情報を管理する情報管理装置であって、ユーザ利用領域に対して任意の情報を書込・読出を行う書込・読出手段と、機密領域に格納されている許諾情報を媒体固有の情報またはそれに基づいて生成された鍵により暗号化して機密領域外に導出する所定情報導出手段とを備えている。

【0018】

ここで、暗号化された許諾情報を、書込・読出手段によりユーザ利用領域に格納する構成とすることができる。

また、ユーザ利用領域に格納されている暗号化された許諾情報を媒体固有の情

報により復号化して機密領域に格納されている許諾情報を更新する所定情報更新手段をさらに備える構成とすることができる。

【0019】

さらに、装置固有の情報を備え、所定情報導出手段は、許諾情報を媒体固有の情報またはそれに基づいて生成された鍵および装置に固有の情報またはそれに基づいて生成された鍵により暗号化するように構成できる。

この場合、ユーザ利用領域に格納されている暗号化された許諾情報を装置に固有の情報またはそれに基づいて生成された鍵および媒体固有の情報により復号化して機密領域に格納されている許諾情報を更新する所定情報更新手段をさらに備える構成とすることができる。

【0020】

また、所定情報導出手段は、暗号化された許諾情報を記録媒体とは異なる第2の記録媒体に送出するように構成できる。

この場合、第2の記録媒体に格納されている暗号化された許諾情報を媒体固有の情報により復号化して機密領域に格納されている許諾情報を更新する所定情報更新手段をさらに備える構成とすることができる。

【0021】

また、第2の記録媒体を駆動する装置は装置固有の情報を備え、所定情報導出手段は、許諾情報を媒体固有の情報またはそれに基づいて生成された鍵および第2の記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵により暗号化するように構成できる。

この場合には、第2の記録媒体に格納されている暗号化された許諾情報を、第2の記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵および媒体固有の情報により復号化して機密領域に格納されている許諾情報を更新する所定情報更新手段をさらに備える構成とすることができる。

【0022】

【発明の実施の形態】

本発明の実施形態について図面を参照して説明する。

〔記録媒体〕

本発明に用いられる記録媒体は、光磁気ディスク（MO）、デジタルビデオディスク（DVD）、フロッピーディスク（FD）、ミニディスク（MD）、その他のユーザによるデータの書き換えが可能な記録媒体であり、例えば光磁気ディスクについてその記録領域を図 1 により説明する。

【0023】

記録媒体 1 は、ユーザによる読み出しは可能であるが書き換えが不可能な第 1 階層 2、外部からの指令による読み出し・書き込みが不可能な第 2 階層 3、ユーザが任意に情報の書き込みを行うことが可能な第 3 階層 4 を有している。第 1 階層 2 には、その媒体について一意に決定される媒体固有番号 2 が格納されている。第 3 階層 4 は、ユーザが任意の情報 7 を格納することが可能な領域であり、ユーザが利用するためのコンピュータプログラム、電子出版物、その他任意のデータを格納するユーザコンテンツ領域である。第 2 階層 3 は、第 3 階層 4 に格納された任意の情報に基づく所定の情報 6 を格納するための領域であり、たとえば、第 3 階層 4 に格納されているコンピュータプログラムや電子出版物などの利用権に基づく許諾情報などが格納される。

〔許諾側の構成〕

記録媒体に電子化データを格納して配布する際に、この電子化データを利用するための利用権をユーザ毎に設定する場合、この電子化データを暗号化して記録媒体に格納する。たとえば、図 2 に示すように、記録媒体 11 に電子化データを格納する場合、第 1 階層 12 に媒体固有番号 15、第 2 階層 13 に利用権に基づく許諾情報 16、第 3 階層 14 に暗号化されたコンテンツ 17 が格納される。ここで、許諾情報 16 は、ユーザの利用権に基づくデータであり、たとえば暗号化されたコンテンツ 17 を復号化するための復号鍵とすることができる。

【0024】

許諾側のコンピュータ 21 では、個別鍵生成手段 22、許諾情報暗号化手段 23、コンテンツ暗号化手段 24、暗号鍵テーブル 25、復号鍵テーブル 26などを備えている。

コンテンツ暗号化手段 24 は、暗号鍵テーブル 25 の暗号鍵によりコンテンツとなるデータ 27 を暗号化し、記録媒体 11 の第 3 階層 14 にコンテンツとして

格納する。暗号鍵テーブル 25 の暗号鍵に対応する復号鍵が復号鍵テーブル 26 に格納される。個別鍵生成手段 22 は、記録媒体 11 の第 1 階層 12 から読み出した媒体固有番号 15 をもとに媒体個別鍵を生成する。許諾情報暗号化手段 23 は、復号鍵テーブル 26 の復号鍵を媒体個別鍵により暗号化して、記録媒体 11 の第 2 階層 13 に許諾情報 16 として格納する。

〔ユーザ側の構成〕

図 1 の記録媒体 1 を駆動するためのユーザ側の駆動装置を図 4 にその概念構成図として示す。

【0025】

駆動装置 31 は、ユーザ利用領域である第 3 階層 4 に任意の情報 7 の書き込み、読み出しを行う書込・読出手段 32 と、機密領域である第 2 階層 3 に格納されている所定の情報 6 を第 1 階層 2 に格納されている媒体固有番号 5 を用いて暗号化し第 2 階層 3 以外の領域に導出する所定情報導出手段 33 とを備えている。所定情報導出手段 33 が許諾情報などの所定の情報を暗号化して導出する場所としては、たとえば、第 3 階層 4 または他の記録媒体が考えられる。暗号化した許諾情報を記録媒体 1 の第 3 階層 4 に格納する場合には、書込・読出手段 32 により任意の情報 7 として格納させることができる。

【0026】

さらに具体的な構成の一例として図 4 に簡略ブロック図を示す。

ユーザ側の駆動装置 41 は、個別鍵生成手段 42、許諾情報復号化手段 43、復号鍵格納部 44、コンテンツ復号化手段 45、復号データ格納部 46、許諾情報暗号化手段 47などを備えている。

個別鍵生成手段 42 は、記録媒体 11 の第 1 階層 12 に格納されている媒体固有番号 15 に基づいて媒体個別鍵を生成するものであって、許諾側の個別鍵生成手段 22 によって生成される個別鍵と同じものを生成する。許諾情報復号化手段 43 は、記録媒体 11 の第 2 階層 13 に格納されている許諾情報 16 を読み出して、個別鍵生成手段 42 により生成された個別鍵により復号化する。許諾情報復号化手段 43 によって復号化された許諾情報は、復号鍵格納部 44 に一時的に格納される。コンテンツ復号化手段 45 は、記録媒体 11 の第 3 階層 14 に格納さ

れているコンテンツ 17を読み出して、復号鍵格納部 44に格納されている復号鍵を用いて復号化し、復号データ格納部 46に格納するものである。

【0027】

許諾情報暗号化手段 47は、第2階層 13の許諾情報 16を読み出して、第1階層 12に格納されている媒体固有番号 12を用いて暗号化する。この場合、媒体固有番号 12をそのまま用いることも可能であり、個別鍵生成手段 42によって生成した個別鍵を用いて暗号化することも可能であり、さらに、媒体固有番号 12に基づいて暗号鍵を生成しこれを用いて暗号化することも可能である。このあと、暗号化した許諾情報を記録媒体 11の第3階層 14内に格納する。

〔コンテンツ格納処理〕

許諾側において記録媒体 11に電子化データを格納する際の動作を図 5にフローチャートとして示す。

【0028】

ステップ S1では、記録媒体 11に格納するコンピュータプログラム、電子出版物、その他の電子化データの作成を行う。ステップ S2では、電子化データを暗号化するための暗号鍵の作成を行う。ステップ S3では、暗号化を行う電子化データと暗号鍵とを対応させて、暗号鍵テーブル 25に格納する。このとき同時に、暗号鍵により暗号化されたデータを復号するための復号鍵が作成され、電子化データと復号鍵とを対応させて復号鍵テーブル 26に格納する。暗号鍵と復号鍵とを共通のものとし、暗号鍵テーブル 25と復号鍵テーブル 26とを1つの鍵管理テーブルとすることも可能である。

【0029】

ステップ S4では、暗号化を行う電子化データに対応する暗号鍵を暗号鍵テーブル 25から取り出す。ステップ S5では、電子化データを暗号鍵により暗号化する。たとえば、DES暗号を用いる場合には、暗号化を行う電子化データに対して換字とビット転置を繰り返して暗号化を行う。ステップ S6では、暗号化された電子化データをコンテンツ 17として、記録媒体 11の第3階層 14に格納する。ステップ S7では、暗号化された電子化データの格納が終了したか否かを判別する。暗号化された電子化データの格納がすべて終了した場合には、ステッ

ブ S 8 に移行する。

【0030】

ステップ S 8 では、記録媒体 11 の第 1 階層 12 から媒体固有番号 15 を読み出して個別鍵を生成する。ステップ S 9 では、コンテンツ 17 として記録媒体 11 に格納した電子化データに対応する復号鍵を復号鍵テーブル 26 から読み出して、ステップ S 8 で生成した個別鍵により暗号化する。コンテンツ 17 として格納した電子化データに対応する復号鍵をすべて暗号化した後、ステップ S 10 において、この暗号化した復号鍵を許諾情報 16 とし記録媒体 11 の第 2 階層 13 に格納する。

〔電子化データの復号化処理〕

記録媒体 11 の第 3 階層 14 に格納されているコンテンツ 17 は、許諾側が作成した暗号鍵によって暗号化されているため、ユーザ側でこれを利用するためには適切な復号鍵により復号化する必要がある。このときの動作を図 6 のフローチャートを用いて説明する。記録媒体 11 が駆動装置 41 に装着されてデータのロード命令がなされると、ステップ S 21 において、記録媒体 11 の第 1 階層 12 から媒体固有番号 15 を読み出す。ステップ S 22 では、媒体固有番号 15 から個別鍵の生成を行う。ここでは、許諾側のステップ S 8 と同じアルゴリズムにより個別鍵を生成する。ステップ S 23 では、記録媒体 11 の第 2 階層 13 に格納されている許諾情報 16 を読み出してこれをステップ S 22 で生成した個別鍵を用いて復号化する。ここで復号化された許諾情報は、コンテンツ 17 を復号化するための復号鍵であり、この復号鍵を第 3 領域 14 に格納されている電子化データと対応させて復号鍵テーブルとし、これを復号鍵格納部 44 に一時的に格納する。

【0031】

ステップ S 24 では、記録媒体 11 の第 3 階層 14 に格納されているコンテンツ 17 を読み込む。ステップ S 25 では、復号鍵格納部 44 に格納されている復号鍵を用いて、読み込んだコンテンツ 17 を復号化する。ステップ S 26 では、復号化されたコンテンツを実行する。

〔許諾情報のバックアップ処理〕

ユーザ側の駆動装置 41 において、記録媒体 11 の第 2 階層 13 に格納されている許諾情報 16 はバックアップデータとして保存される。この処理を図 7 を用いて説明する。

【0032】

ステップ S31 では、記録媒体 11 の第 2 階層 13 に格納されている許諾情報 16 を読み出す。ステップ S32 では、読み出した許諾情報 16 を媒体固有番号 15 によって暗号化する。このとき、ステップ 22 により生成された個別鍵を用いて許諾情報 16 の暗号化を行うことも可能であり、他のアルゴリズムにより媒体固有番号 15 を暗号化した鍵を用いて暗号化するように構成することも可能である。ステップ S33 では、暗号化された許諾情報 16 を記録媒体 11 の第 3 階層 14 内に格納する。

【0033】

このような構成の場合、第 3 階層 14 内に許諾情報 16 のバックアップが保存されているため、第 2 階層 13 の許諾情報 16 が破壊されたときに、第 3 階層 14 内のバックアップデータを読み出して第 2 階層 13 に戻せば、許諾情報 16 の再発行を待たずにコンテンツ 17 を利用することが可能となる。また、第 3 階層 14 に保存されている許諾情報は、媒体固有番号 15 によって暗号化されているため、記録媒体 11 の第 3 階層 14 に格納されている内容がそっくりコピーされても、元の許諾情報 16 を復元することは困難であり、コンテンツ 17 の不正利用を防止することができる。

〔他の実施形態〕

(A) 記録媒体 11 の第 2 階層 13 に格納されている許諾情報 16 が破壊された場合に、第 3 階層 14 に保存しておいた許諾情報のバックアップデータを用いて許諾情報 16 を復元する機能が、記録媒体 11 を駆動する駆動装置に備わっている場合について説明する。図 8 は、このような駆動装置 51 の制御ブロック図であり、個別鍵生成手段 42、許諾情報復号化手段 43、復号鍵格納部 44、コンテンツ復号化手段 45、復号データ格納部 46 および許諾情報暗号化手段 47 は、図 4 に示した実施形態と同様であり説明を省略する。

【0034】

許諾情報更新手段 52 は、記録媒体 11 の第 3 階層 14 に保存されている暗号化された許諾情報を読み出して、これを第 1 階層 12 に格納されている媒体固有番号 15 によって復号化する。ここで、第 3 階層 14 に保存されている許諾情報が個別鍵生成手段 42 によって生成された個別鍵により暗号化されている場合には、復号化に用いる鍵はこの個別鍵を用いることとなる。このあと、復号化された許諾情報は、許諾情報 16 として記録媒体 11 の第 2 階層 13 に格納される。

【0035】

この実施形態の動作について図 9 にフローチャートとして示す。

ステップ S41 では、記録媒体 11 の第 3 階層 14 に格納されている暗号化された許諾情報を読み出す。ステップ S42 では、読み出した暗号化された許諾情報を媒体固有番号 15 によって復号化する。このとき、ステップ 22 により生成された個別鍵を用いて許諾情報の復号化を行うことも可能であり、他のアルゴリズムにより媒体固有番号 15 を暗号化した鍵を用いて暗号化されている場合には、この鍵を用いて復号化を行う。ステップ S43 では、復号化された許諾情報を記録媒体 11 の第 2 階層 13 に許諾情報 16 として格納する。

【0036】

このことにより、記録媒体 11 の第 2 階層 13 に格納されている許諾情報 16 はなんらかの障害により破壊された場合には、第 3 階層 14 にバックアップデータとして保存されている暗号化された許諾情報を用いて復元することが可能である。この復元処理は、駆動装置 51 内で処理されるため、許諾情報 16 が外部に出力されることがなく、この情報を不正に利用することは不可能となっている。

(B) 記録媒体 11 を駆動するための駆動装置に固有の装置固有番号によりさらに暗号化を行う場合の実施形態を図 10～図 12 に示す。

【0037】

図 10 に示すように、駆動装置 61 において、個別鍵生成手段 42、許諾情報復号化手段 43、復号鍵格納部 44、コンテンツ復号化手段 45、復号データ格納部 46 および許諾情報暗号化手段 47 は、図 4 に示した実施形態と同様であり説明を省略する。また、駆動装置 61 は装置固有番号を格納する装置固有番号格納部 62 を備えている。さらに、第 2 許諾情報暗号化手段 63 を備えている。こ

の第2許諾情報暗号化手段63は、許諾情報暗号化手段47で媒体固有番号15によって暗号化された許諾情報を、さらに装置固有番号によって暗号化するものである。この第2許諾情報暗号化手段63によって暗号化された許諾情報は、記録媒体11の第3階層14内に格納される。

【0038】

また、駆動装置61は許諾情報更新手段64を備えている。この許諾情報更新手段64は、記録媒体11の第3階層14に保存されている暗号化された許諾情報を読み出して、これを装置固有番号格納部62に格納されている装置固有番号により復号化する第1許諾情報復元手段65と、第1許諾情報復元手段65が復号化した許諾情報を記録媒体11の第1階層12に格納されている媒体固有番号15によって復号化する第2許諾情報復元手段66とを備えている。復元された許諾情報は、記録媒体11の許諾情報16として第2階層13に格納される。

【0039】

記録媒体11に格納されている許諾情報16のバックアップを保存する際には、図11に示す手順で行われる。

まず、ステップS51では、記録媒体11の第2階層13に格納されている許諾情報16を読み出す。ステップS52では、読み出した許諾情報16を第1階層12に格納されている媒体固有番号15によって暗号化する。ステップS53では、媒体固有番号15によって暗号化された許諾情報を、装置固有番号格納部62に格納された装置固有番号により暗号化する。このあと、暗号化された許諾情報をステップS54において第3階層14内に格納する。

【0040】

記録媒体11に格納されている許諾情報16が破壊された場合には、図12に示す手順で許諾情報の復元を行う。

ステップS61では、記録媒体11の第3階層14に格納されている暗号化された許諾情報を読み出す。ステップS62では、読み出した暗号化された許諾情報を装置固有番号により復号化する。ステップS63では、装置固有番号により復号化された許諾情報を媒体固有番号15によって復号化する。ステップS64では、復号化された許諾情報を記録媒体11の第2階層13に許諾情報16とし

て格納する。

【0041】

このように構成した場合には、許諾情報16のバックアップデータが媒体固有番号15によって暗号化され、さらに駆動装置61の装置固有番号によって暗号化されているため、データの違法コピーを行っても利用することができず、著作権保護をすることができる。また、記録媒体11の許諾情報16が破壊されたとしても、この駆動装置61を用いて復元することが可能であり、正規のユーザであれば再発行を待たずにコンテンツの利用が可能となる。

【0042】

装置固有番号は、記録媒体11を駆動するための駆動装置61に固有の装置番号としたが、ユーザ側で使用しているコンピュータに固有の装置番号を利用することも可能である。また、許諾情報16のバックアップデータを保存する際に装置固有番号によって暗号化した後、媒体固有番号15によって暗号化して格納することも可能であり、これを復元する場合は媒体固有番号15によって復号化した後に装置固有番号によって復号化することとなる。

(C) 許諾情報16のバックアップデータを他の記録媒体に保存しておくことも可能である。このような実施形態について、図13～図15に基づいて説明する。

【0043】

記録媒体11を駆動するための駆動装置71は、第2の記録媒体83を駆動するための駆動装置81と接続されており、媒体間のデータのやりとりが可能となっている。駆動装置81は、たとえば、フロッピーディスクドライブ(FDD)、ハードディスクドライブ(HDD)、ミニディスク(MD)、光磁気ディスク(MO)、デジタルディスクドライブ(DVD)などが採用され、装置固有番号を格納するための装置固有番号格納部82を備えており、この装置固有番号を電子データとして出力することが可能となっている。

【0044】

記録媒体11を駆動する駆動装置71において、個別鍵生成手段42、許諾情報復号化手段43、復号鍵格納部44、コンテンツ復号化手段45、復号データ

格納部 46 および許諾情報暗号化手段 47 は、図 4 に示した実施形態と同様であり説明を省略する。駆動装置 71 は、さらに、第 2 許諾情報暗号化手段 72 と、許諾情報更新手段 73 とを備えている。第 2 許諾情報暗号化手段 72 は、許諾情報暗号化手段 47 によって暗号化された許諾情報を、さらに駆動装置 81 の装置固有番号によって暗号化する。このあと、暗号化された許諾情報を第 2 の記録媒体 83 に格納する。

【0045】

許諾情報更新手段 73 は、第 2 の記録媒体 83 に保存されている暗号化された許諾情報を読み出して、これを装置固有番号格納部 82 に格納されている装置固有番号により復号化する第 1 許諾情報復元手段 74 と、第 1 許諾情報復元手段 74 が復号化した許諾情報を記録媒体 11 の第 1 階層 12 に格納されている媒体固有番号 15 によって復号化する第 2 許諾情報復元手段 75 とを備えている。復元された許諾情報は、記録媒体 11 の許諾情報 16 として第 2 階層 13 に格納される。

【0046】

記録媒体 11 に格納されている許諾情報 16 のバックアップを保存する際には、図 14 に示す手順で行われる。

まず、ステップ S71 では、記録媒体 11 の第 2 階層 13 に格納されている許諾情報 16 を読み出す。ステップ S72 では、読み出した許諾情報 16 を第 1 階層 12 に格納されている媒体固有番号 15 によって暗号化する。ステップ S73 では、媒体固有番号 15 によって暗号化された許諾情報を、第 2 の記録媒体 83 を駆動するための駆動装置 81 の装置固有番号により暗号化する。このあと、暗号化された許諾情報をステップ S74 において第 3 階層 14 内に格納する。

【0047】

記録媒体 11 に格納されている許諾情報 16 が破壊された場合には、図 15 に示す手順で許諾情報 16 の復元処理が行われる。

ステップ S81 では、第 2 の記録媒体 83 に格納されている暗号化された許諾情報を読み出す。ステップ S82 では、読み出した暗号化された許諾情報を第 2 の記録媒体 83 を駆動する駆動装置 81 の装置固有番号により復号化する。ステ

ップ S 8 3 では、装置固有番号により復号化された許諾情報を媒体固有番号 1 5 によって復号化する。ステップ S 8 4 では、復号化された許諾情報を記録媒体 1 1 の第 2 階層 1 3 に許諾情報 1 6 として格納する。

【0048】

このように構成した場合には、許諾情報 1 6 のバックアップデータを記録媒体 1 1 と切り離して管理することができ、高いセキュリティを維持することができる。また、複数の記録媒体について、その許諾情報をユーザ側で管理することが可能であり、許諾情報がなんらかの形で破壊されても、ユーザ側で対応することが可能である。ここでも、許諾情報 1 6 を暗号化する際に、装置固有番号で暗号化した後、媒体固有番号で暗号化するように構成してもよい。この場合には、これを復元する際には、媒体固有番号で復号化した後に装置固有番号で復号化することとなる。

(D) ケーブルテレビやインターネットなどにおいて暗号化したデータを放送し、これをユーザ側で記録媒体に記録させる場合に、上述のような方法を適用することができる。たとえば、ユーザ側から暗号化データを記録した記録媒体の媒体固有番号を放送局に送信させ、その媒体固有番号で暗号化された復号鍵をユーザに送信する。ユーザ側の装置では、この復号鍵を記録媒体の第 2 階層の許諾情報として格納する。さらに、この許諾情報を媒体固有番号によって暗号化して第 3 階層に格納する。

【0049】

記録媒体上のコンテンツを利用する場合には、媒体固有番号により許諾情報を復号化して復号鍵を生成し、暗号化されたデータを復号化すればよい。この場合にも、他の記録媒体にコンテンツをそのままコピーしても、許諾情報が媒体固有番号によって暗号化されており、復号化することが困難である。また、バックアップデータを用いて許諾情報を復元することが可能であり、許諾情報が破壊された場合であっても、ユーザ側で復元することが可能である。

【0050】

【発明の効果】

本発明によれば、記録媒体の所定の領域に格納された所定の情報を、媒体固有

の情報によって暗号化して導出しており、他の記録媒体にコピーしても、これを復号化することが困難である。例えば、ソフトウェアや出版物などの電子化データを格納する際に、この電子化データを暗号鍵により暗号化して格納しておき、これを復号するための復号鍵をこの記録媒体に固有の情報で暗号化してユーザのアクセス不可能な領域に格納しておけば、暗号化するための暗号鍵をユーザ個々に変える必要がなく、共通の暗号鍵を用いて暗号化して格納できる。暗号化された復号鍵は、さらに媒体固有の情報を用いて暗号化されて、所定の領域外に導出するように構成しているため、ユーザのバックアップとして保存しておくことが可能である。この保存されたバックアップデータは、媒体固有の情報により暗号化されているため、これを他の記録媒体にコピーしても復号化することが困難であり、電子化データを復号するための復号鍵を得ることは困難である。また、ユーザはこのバックアップデータを用いて復号鍵を復元することができるため、データがなんらかの障害が破壊された場合であっても、再発行の手続きを省略することが可能となる。

【図面の簡単な説明】

【図1】

本発明に用いられる記録媒体の記録領域を示す概念図。

【図2】

許諾側における簡略ブロック図。

【図3】

本発明の概念構成図。

【図4】

1 実施形態の簡略ブロック図。

【図5】

コンテンツ格納処理の制御フローチャート。

【図6】

復号化処理の制御フローチャート。

【図7】

バックアップ処理の制御フローチャート。

【図 8】

他の実施形態の簡略ブロック図。

【図 9】

許諾情報更新処理のフローチャート。

【図 10】

他の実施形態の簡略ブロック図。

【図 11】

その制御フローチャート。

【図 12】

その制御フローチャート。

【図 13】

他の実施形態の簡略ブロック図。

【図 14】

その制御フローチャート。

【図 15】

その制御フローチャート。

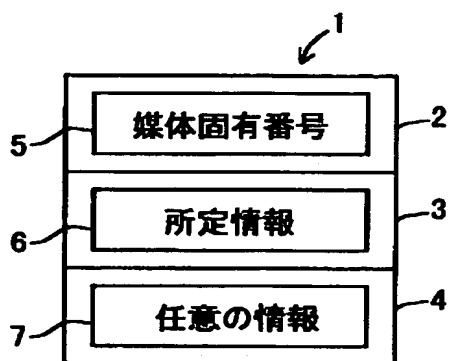
【符号の説明】

- 1 記録媒体
- 2 第 1 階層
- 3 第 2 階層
- 4 第 3 階層
- 5 媒体固有番号
- 6 所定の情報
- 7 任意の情報
- 1 1 記録媒体
- 1 2 第 1 階層
- 1 3 第 2 階層
- 1 4 第 3 階層
- 1 5 媒体固有番号

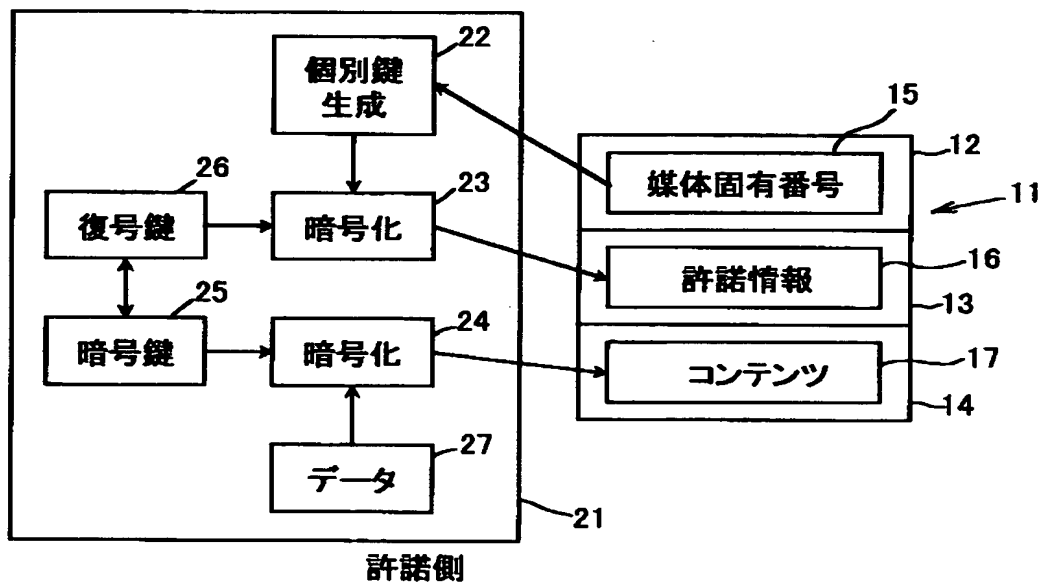
- 16 許諾情報
- 17 コンテンツ
- 21 許諾側コンピュータ
- 22 個別鍵生成手段
- 23 許諾情報暗号化手段
- 24 コンテンツ暗号化手段
- 25 暗号鍵テーブル
- 26 復号鍵テーブル
- 31 駆動装置
- 32 書込・読出手段
- 33 所定情報導出手段
- 41 駆動手段
- 42 個別鍵生成手段
- 43 許諾情報復号化手段
- 44 復号鍵格納部
- 45 コンテンツ復号化手段
- 46 データ格納部
- 47 許諾情報暗号化手段
- 52 許諾情報更新手段
- 83 第2の記録媒体

【書類名】 図面

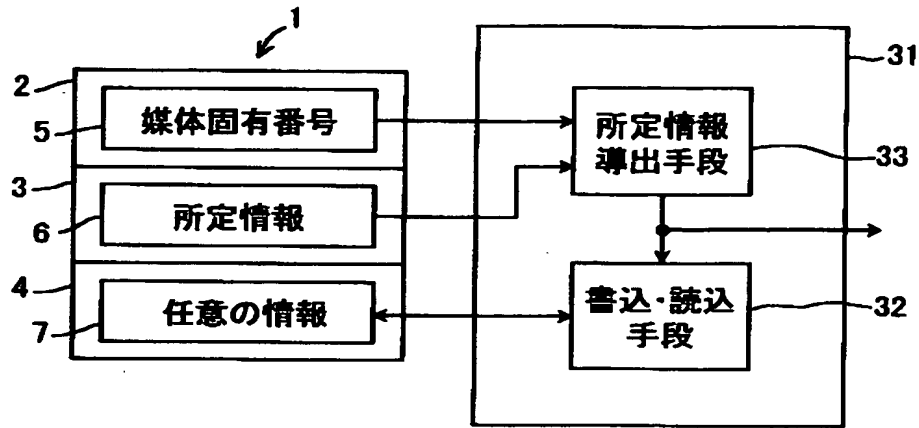
【図 1】



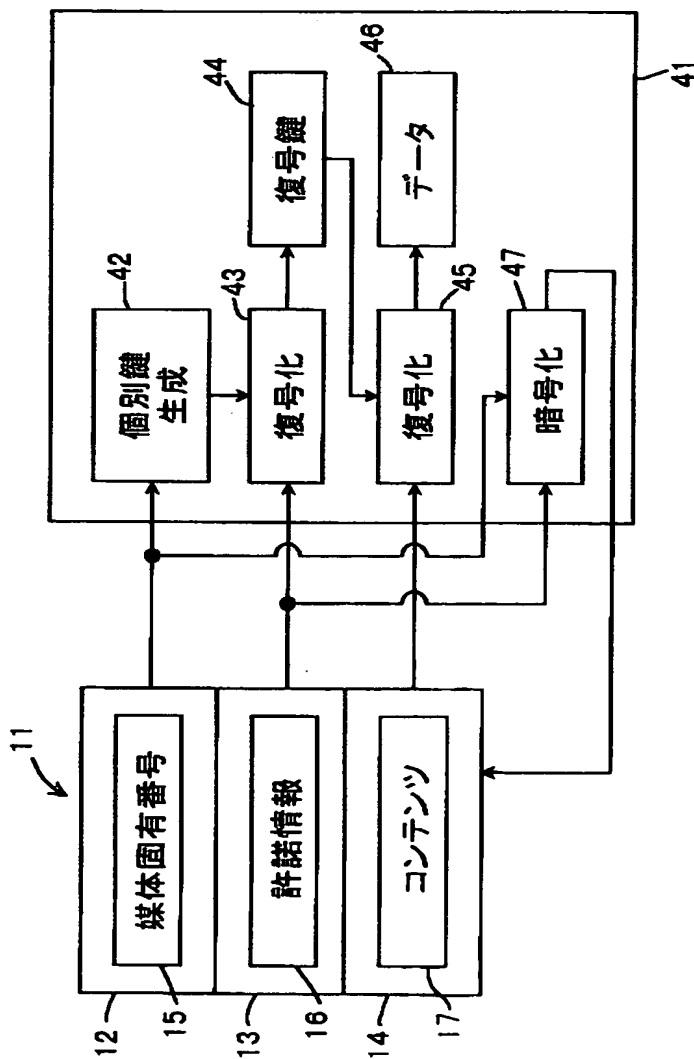
【図 2】



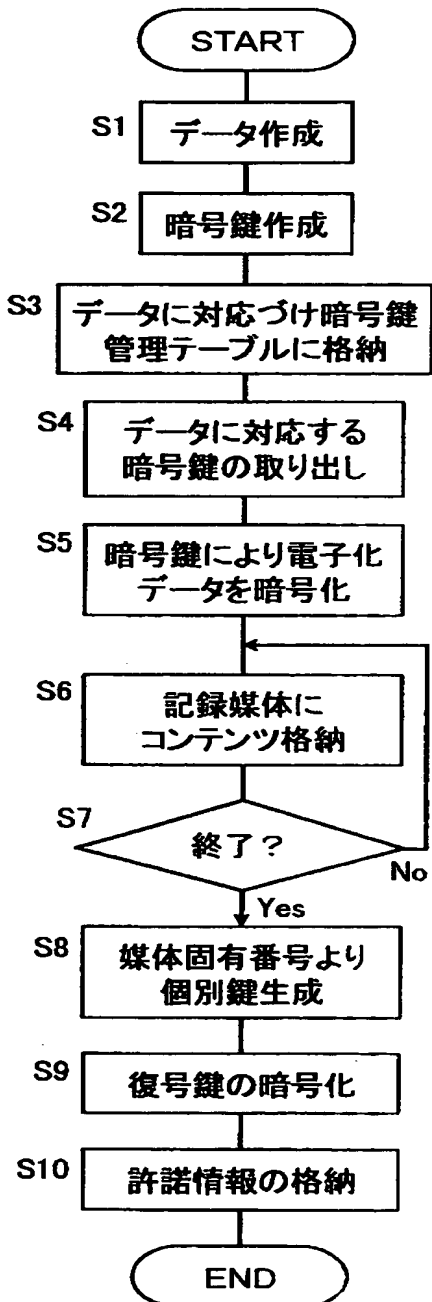
【図 3】



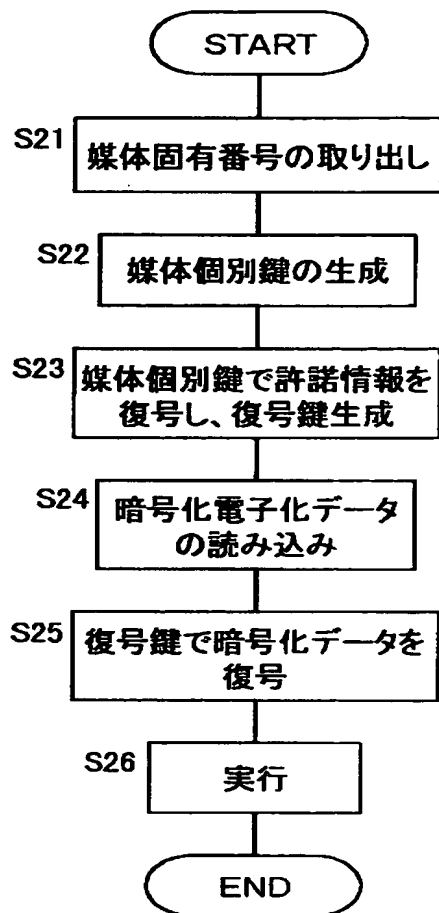
【図 4】



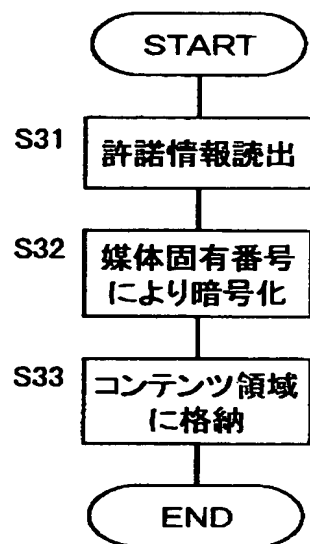
【図 5】



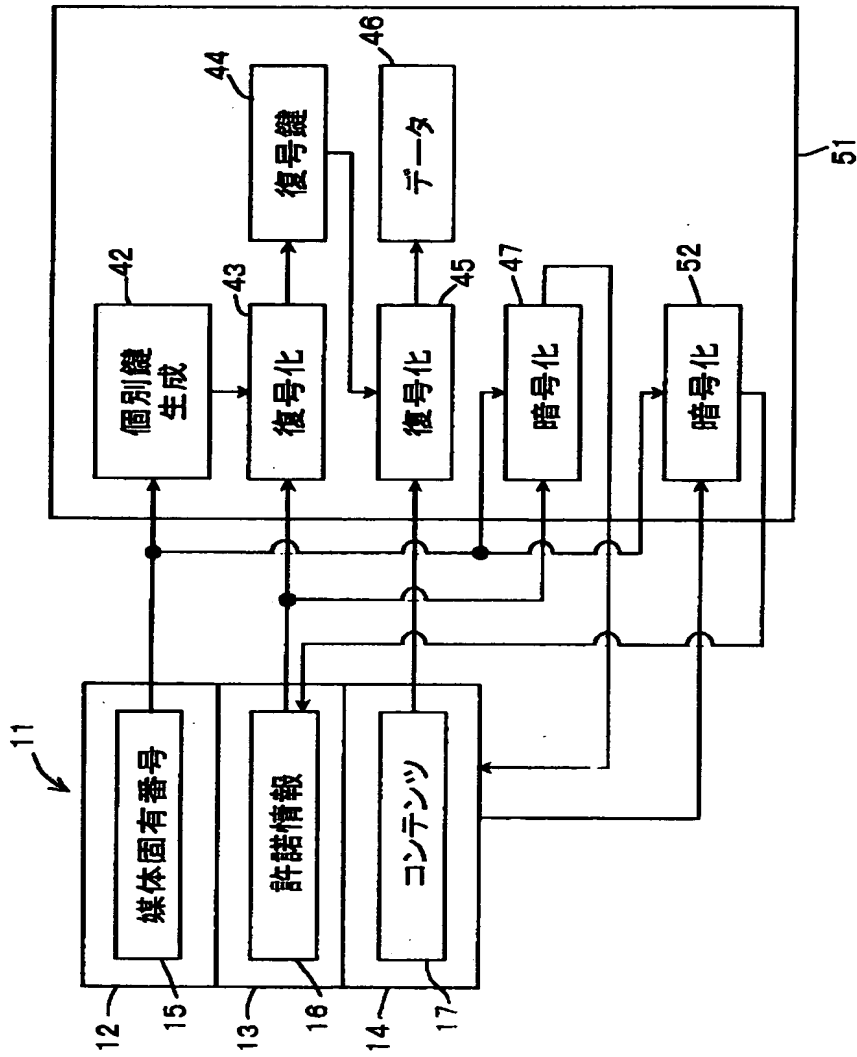
【図 6】



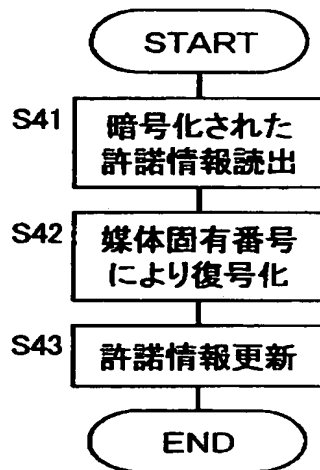
【図 7】



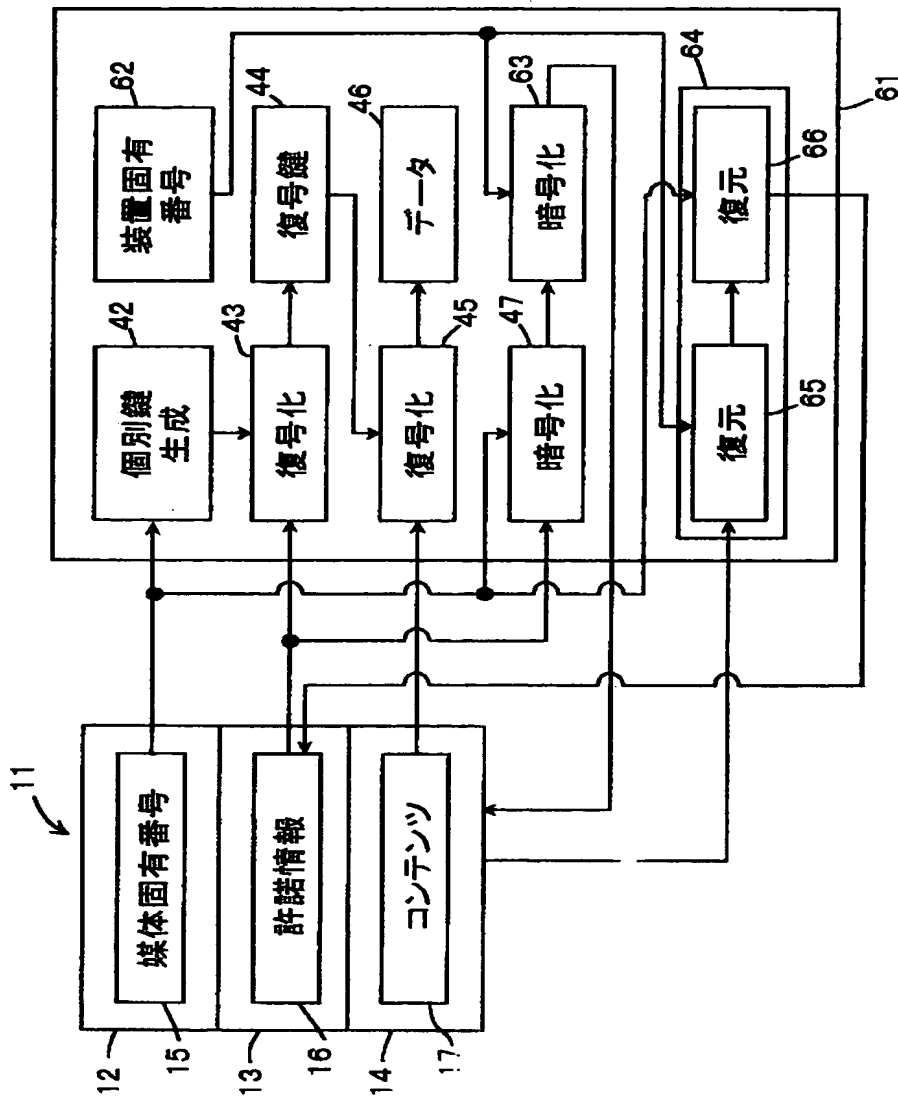
【図 8】



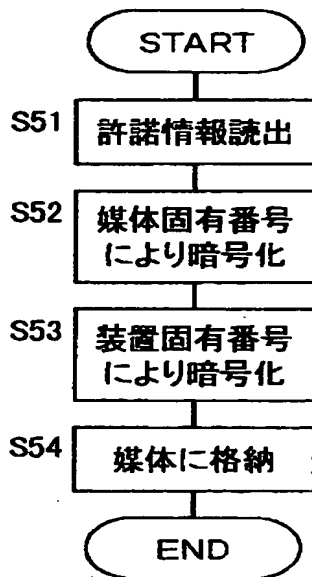
【図 9】



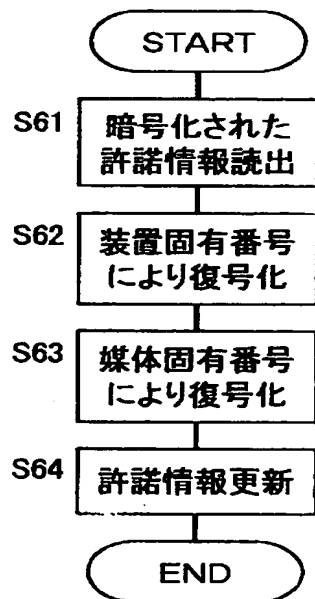
【図 10】



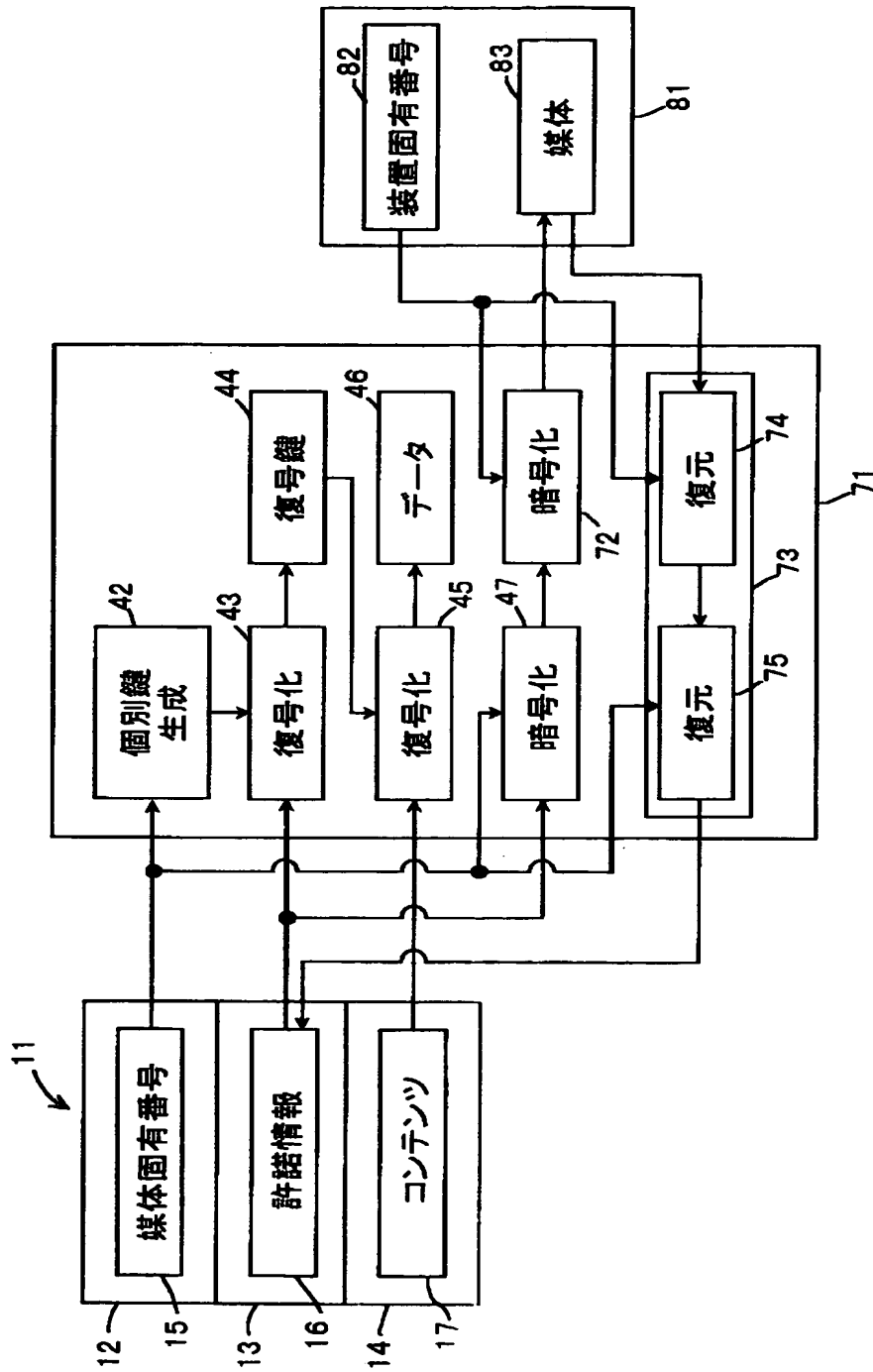
【図 1 1】



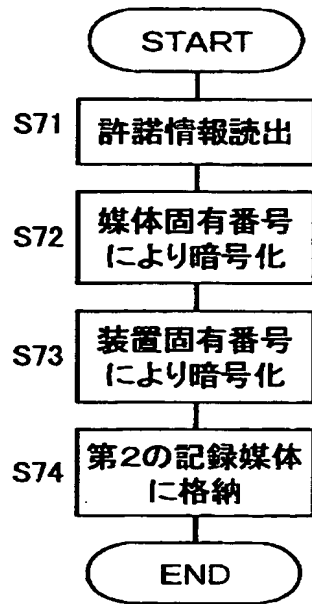
【図 1 2】



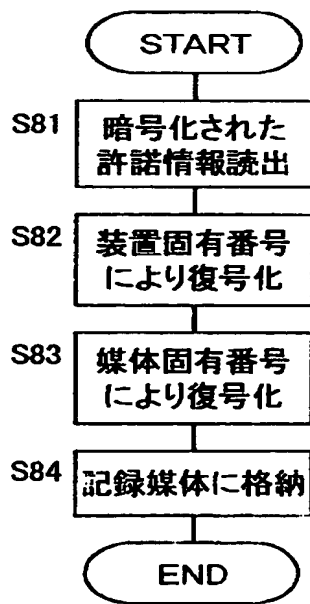
【図 13】



【図 14】



【図 15】



【書類名】 要約書

【要約】

【課題】 記録媒体上に格納された電子化データを利用するために必要な許諾情報がなんらかの障害により破壊された場合であっても、ユーザがバックアップ情報を用いてこれを復帰させることが可能な情報管理方法を提供する。

【解決手段】 記録媒体のユーザによるアクセスが不可能な第2階層に格納されている許諾情報を読み出して（ステップS31）、記録媒体の媒体固有番号によって暗号化し（ステップS32）、暗号化した許諾情報を記録媒体のユーザが任意に利用できる第3階層に格納する（ステップS33）。

【選択図】 図7

【書類名】 職権訂正データ
【訂正書類】 特許願

<認定情報・付加情報>

【特許出願人】
【識別番号】 000005223
【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号
【氏名又は名称】 富士通株式会社
【代理人】 申請人
【識別番号】 100094145
【住所又は居所】 大阪市都島区片町1丁目5番13号 大手前センチュリービル 新樹合同特許事務所
【氏名又は名称】 小野 由己男
【選任した代理人】
【識別番号】 100094167
【住所又は居所】 大阪市都島区片町1丁目5番13号 大手前センチュリービル 新樹合同特許事務所
【氏名又は名称】 宮川 良夫
【選任した代理人】
【識別番号】 100106367
【住所又は居所】 大阪市都島区片町1丁目5番13号 大手前センチュリービル 新樹合同特許事務所
【氏名又は名称】 稲積 朋子

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日	1996年 3月26日
[変更理由]	住所変更
住 所	神奈川県川崎市中原区上小田中4丁目1番1号
氏 名	富士通株式会社